INTRODUCTION

This report updates the Committee's February 1999 report on the status of Y2K preparedness in the U.S. and the rest of the world. It describes these Y2K efforts in terms of the eight critical infrastructure and industry sectors identified when the Committee was formed in April 1998. During 1999, the Committee found it necessary to add international preparedness and personal preparedness to these original sectors.

> ***"THE LONGER WE DELAY IN FIXING THE COMPUTER PROBLEM, THE MORE COSTLY THE SOLUTION AND THE MORE DIRE THE CONSEQUENCES. THE COMPUTER HAS BEEN A BLESSING; IF WE DO NOT ACT IN A TIMELY FASHION, HOWEVER, IT COULD BECOME THE CURSE OF THE AGE."***
>
> ***-- SENATOR MOYNIHAN***

Our February 1999 report contained a wealth of detailed information on the nature of the Y2K problem. Since so much has been written on Y2K in the interim, and since public awareness of the issue is high, we will not re-explain the nature of the Y2K problem. We simply refer those seeking additional Y2K information to the Committee's Web site at http://y2k.senate.gov or http://www.senate.gov/~y2k/, or to the Committee itself.[1]

For purposes of this report, we find it sufficient to say that the Y2K problem is very real and will indeed have a profound impact on us. Its least severe impact will be disruptions to supply chains that may affect the availability--and thus the price--of some goods and services. In worst case scenarios, there may be some electric power, gas, telecommunications or other infrastructure outages in some locations, particularly where a utility started too late or did not aggressively address the problem. Unfortunately, no one knows for sure exactly where those outages will be or how long they will last.

The fact that we live in an interconnected world adds to the difficulty in accurately predicting the exact nature, location, or severity of the Y2K problem. The complicated nature of this interconnectedness can be illustrated by describing the two general classes of equipment affected by the Y2K problem. The first class comprises business systems or mainframe systems. These computers perform a variety of data-intensive calculations such as balancing accounts, making payments, tracking inventory, ordering goods, managing personnel, scheduling resources, and so forth.

The second class of equipment has several common names, including embedded chips, embedded processors, and embedded control systems. Many aspects of modern society rely on microchip-enhanced technology to control or augment operations. Examples are ubiquitous. Automatic teller machines,, toll collection systems, security and fire detection systems, oil and gas pipelines, consumer electronics, transportation vehicles, manufacturing process controllers, military systems, medical devices, and telecommunications equipment all depend on embedded chip technology.

Y2K-related failures in business systems may cause an enterprise to lose partial or complete control of critical processes. In the private sector, loss of business systems means a firm may have difficulty managing its finances, making or receiving payments, or tracking inventory, orders, production or deliveries. In the public sector, government organizations may be severely hindered in performing basic functions such as paying retirement and medical benefits, maintaining military readiness, responding to state and local emergencies, controlling air traffic, collecting taxes and customs, and coordinating law enforcement efforts.

Y2K problems in embedded systems may adversely affect public health and safety. Problems have already been detected in medical treatment devices, water and electricity distribution and control systems, airport runway lighting, and building security systems.[2] Other areas of concern are pipeline control systems and chemical and pharmaceutical manufacturing processes.

It is also worth reiterating that not all of the Y2K problems will occur on January 1, 2000. Indeed, some Y2K problems have already surfaced. The Gartner Group, an information technology research company, has developed a model to predict the rate of occurrence of Y2K problems. This prediction is based on data collected quarterly from more than 15,000 firms and government organizations in 87 countries. Gartner estimates a rapid increase in problems in 1999 with a peak sometime after January 1, 2000. Problem occurrences will drop off after 2000, but will still occur for another 3-5 years at a lower level.

Those who remain skeptical about the seriousness of the Y2K problem need only examine the amount of money being spent to address it. Although no one knows the exact amount, Capers Jones, of Software Productivity Research, Inc., has arrived at a worldwide estimated cost of more than $1.6 trillion, including more than $300 billion in potential litigation and damages.[3]

A sense of the scale of these costs can be gained by looking at the Y2K disclosures to the Securities and Exchange Commission (SEC) for some Fortune 100 companies as shown in Figure 1.

Figure 1. Y2K Repair Estimates[4]

Company	*Estimate (Millions)*
ATT	$756
Cendant	$55
General Motors	$564-624
McDonald’s	$80
Merrill Lynch	$520
Xerox	$183

LESSONS LEARNED FROM Y2K

As with any global challenge, the Y2K problem has been a valuable learning experience. The full scope of some lessons will not be ascertainable until well into the next century, but other lessons, positive and negative, have already been learned.

On the positive side, the Y2K problem has caused organizations worldwide to reexamine their use of information technology and, in some cases, to streamline operations. History teaches us that a more efficient use of technology can lead to continued economic growth.

On the negative side, Y2K has greatly heightened our awareness of the vulnerabilities that the extensive and interconnected use of technology creates in our critical infrastructures—the computerized and physical services essential to the basic functioning of the economy and the government.

> ***Mr. President,***
>
> ***I write to alert you to a problem which could have extreme negative economic consequences . . . the Year 2000 time bomb. I have a recommendation. A Presidential aide should be appointed . . . (to ensure) that all federal agencies . . . be date compliant by January 1, 1999.***
>
> ***-Senator Moynihan***
> ***July 31, 1996, letter to President Clinton***

In the past, many of these key infrastructures or sectors were separate. However, advances in information technology have allowed many of these systems to be interconnected and linked through networks. The Committee has approached critical infrastructures by examining the Y2K work occurring both vertically within specific sectors and horizontally across different interrelated sectors, such as banking and telecommunications.

At the urging of Senator Moynihan, the President issued Executive Order No. 13010 creating the President's Commission on Critical Infrastructure Protection. Although the Commission was not given the specific task of studying Y2K, it recognized the potential for Y2K to cause long-term problems in the infrastructures. For example, many organizations have entered into contracts with outside firms to work on sensitive systems. In some cases, organizations have sent code overseas to foreign firms. The correction of code overseas could lead to increased incidents of corporate espionage and intentional cyber disruptions. The broad scope of Y2K corrections could allow an adversary to build an exceptional understanding of sensitive systems, enabling it to design a subtle or comprehensive attack against critical systems.[5]

It is vital that the owners, operators, and regulators of the nation’s critical systems understand that Y2K may provide opportunities for those with malicious intent. Sandia National Laboratories warned the Committee:

"Thinking that we will be so preoccupied with Y2K that we would not notice deliberate malicious intent, terrorists, hackers and other criminals might see Y2K as a prime opportunity to attack pieces of our infrastructure. Or they might use Y2K-induced infrastructure failures as cover for theft, arson, bombings, etc. We must be watchful of such groups in the months leading up to Y2K and we must be especially careful when monitoring the crisis as it occurs to discern deliberate intent."[6]

Critical infrastructure security problems transcend Y2K. Current national security and emergency preparedness policies are not designed for the challenges of the information age. The U.S. needs a system or process whereby the government can coordinate responses with the privately owned and operated critical infrastructures. We must build the broad-based contingency plans necessary to ensure that the national security and emergency preparedness posture of the U.S. is not compromised by Y2K, and we must remain ready to mitigate Y2K's potential economic, emergency, and security effects.

Y2K presents an opportunity to educate ourselves about the nature of 21st century threats. Technology has given our nation many advantages, but has also created many new vulnerabilities. Recognizing shifts in the technological topography of the nation requires vision. Reverting to a world without microchips or technology-dependent systems is not only undesirable, but impossible. Instead, we, as a nation and as individuals, need to carefully consider our reliance on information technology and the consequences of interconnectivity, and must work to protect that which we have taken for granted.

CHARTER OF THE SPECIAL COMMITTEE

On April 2, 1998, the U.S. Senate unanimously voted to establish a new committee to address the Y2K problem. Senate Majority Leader Lott named Senator Bennett to serve as its Chairman. Committee membership has changed slightly since its inception and currently includes:

- Senator Robert F. Bennett, Chairman (R-Utah)
- Senator Christopher J. Dodd, Vice-Chairman (D-Connecticut)
- Senator Jon Kyl (R-Arizona)
- Senator Richard G. Lugar (R-Indiana)
- Senator Gordon Smith (R-Oregon)
- Senator Daniel Patrick Moynihan (D-New York)
- Senator John Edwards (D-North Carolina)

- Senator Ted Stevens (R-Alaska) *ex-officio*
- Senator Robert C. Byrd (D-West Virginia) *ex-officio*

The Committee initially prioritized its activities into the following areas of concern:

1. Utilities
2. Healthcare
3. Telecommunications
4. Transportation
5. Financial Services
6. General Government
7. General Business
8. Litigation

As 1999 progressed, the Committee found it necessary to add international preparedness and personal preparedness to these original sectors.

COMMITTEE'S PURPOSE

The Committee's purpose has remained constant:

(1) to study the impact of the Y2K problem on the executive and judicial branches of the federal government, state governments, and private sector operations in the U.S. and abroad;

(2) to make such findings of fact as are warranted and appropriate; and

(3) to make such recommendations, including recommendations for new legislation and amendments to existing laws and any administrative or other actions, as the Committee determines to be necessary or desirable.

No proposed legislation shall be referred to the Committee, and the Committee does not have the power to report by bill or otherwise have legislative jurisdiction.[7]

Because the Committee does not have legislative authority, each of its members was carefully selected based on his membership on other committees, such as the Senate Judiciary, Armed Services, and Government Affairs Committees.

The Committee's enabling legislation provides that the Committee will exist until February 29, 2000, after which it will permanently disband.

[1] Transcripts and/or statements from each Committee hearing cited in this report can be found on the Committee's Web site.

[2] "Year 2000 Recession?", Edward Yardeni, Version 9.1, Nov. 2, 1998, Chapter 3, http://www.yardeni.com/y2kbook.html.

[3] "The Global Economic Impact of the Year 2000 Software Problem," Capers Jones, Version 5.2, Jan. 23, 1997, Software Productivity Research, Burlington, MA, pp. 57-58.

[4] These estimates are derived from the firms' second quarter 1999 10-Q filings, which can be found in the EDGAR database through http://www.sec.gov, the Securities and Exchange Commission's Web site.

[5] Critical Foundations: Protecting America's Critical Infrastructures, President's Commission on Critical Infrastructure Protection Report, Oct. 1997.

[6] Testimony of Sandia National Laboratories before the U.S. Senate Special Committee on the Year 2000 Technology Problem, July 31, 1998, “Telecommunications and Y2K: Communicating the Challenge of the Year 2000,” S. Hrg. 105-692, p. 138.

[7] S. Res. 208, (105th Cong., 2nd Sess..): To establish a special committee of the Senate to address the year 2000 technology problem.